

**DAMPAK SERANGAN *HACKING* CHINA TERHADAP
KEAMANAN *CYBER* (*CYBER SECURITY*) AMERIKA
SERIKAT**

SKRIPSI

*Disusun dan diajukan untuk memenuhi salah satu syarat
memperoleh gelar Sarjana Ilmu Politik (S.IP) Strata-1*



Oleh :
NURUS SHOIMAH
09260148

**JURUSAN ILMU HUBUNGAN INTERNASIONAL
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS MUHAMMADIYAH MALANG
2016**

LEMBAR PENGESAHAN

Nama : Nurus Shoimah
NIM : 09260148
Jurusan : Hubungan Internasional
Fakultas : Ilmu Sosial dan Ilmu Politik
Judul Skripsi : Dampak Serangan *Hacking* China Terhadap Keamanan
Cyber (Cyber Security) Amerika Serikat

Telah Dipertahankan Dihadapan Dewan Penguji Ujian Skripsi

Fakultas Ilmu Sosial dan Ilmu Politik

Jurusan Ilmu Hubungan Internasional

Dan dinyatakan LULUS

Pada hari: Senin, 01 Agustus 2016

Tempat: Kantor Jurusan Hubungan Internasional Lt.6 GKB I

Mengesahkan,
Dekan FISIP-UMM

Dr. Asep Nurjaman, M.Si

Dewan Penguji:

- | | | |
|------------------|-------------------------------|-----|
| 1. Penguji I | : Helmia Asyathri, M.Sos | () |
| 2. Penguji II | : Havidz Ageng Prakoso, MA | () |
| 3. Pembimbing I | : Gonda Yumitro, MA | () |
| 4. Pembimbing II | : Ruli Inayah Ramadhoan, M.Si | () |

KATA PENGANTAR

Segala puji bagi Allah SWT, yang telah memberikan rahmat dan hidayah-Nya, sehingga skripsi ini dapat terselesaikan. Penulis menyadari banyak studi yang telah meneliti dan membahas tentang permasalahan *cyber* teknologi, *Cyber War* dan *Cyber Security*.

Dengan rahmat Allah S.W.T penulis dapat menyelesaikan skripsi ini dengan judul: “**Dampak Serangan *Hacking* China Terhadap Keamanan *Cyber* (*Cyber Security*) Amerika Serikat**”. Penelitian ini diajukan untuk memenuhi salah satu syarat untuk mendapatkan gelar sarjana Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik. Penulis menyadari bahwa penyusunan skripsi ini masih banyak terdapat kekurangan dan masih jauh dari kesempurnaan, hal ini dikarenakan keterbatasan kemampuan yang penulis miliki.

Atas segala kekurangan dan ketidaksempurnaan skripsi ini, penulis sangat mengharapkan masukan, kritik dan saran yang bersifat membangun kearah perbaikan dan penyempurnaan skripsi ini. Cukup banyak kesulitan yang penulis temui dalam penulisan skripsi ini, tetapi penulis dapat atasi dan selesaikan dengan baik. Pihak-pihak yang banyak membantu dalam penyelesaian penelitian ini, khususnya dukungan orang tua, dosen-dosen pembimbing dan teman-teman yang membantu menyelesaikan skripsi ini, penulis mengucapkan banyak terima kasih.

Penulis

Nurus Shoimah

09260148

DAFTAR ISI

| | |
|--|--------------|
| COVER | i |
| Lembar Persetujuan Skripsi | ii |
| Lembar Pengesahan Skripsi | iii |
| Berita Acara Bimbingan Skripsi | iv |
| Pernyataan Orisinalitas..... | v |
| Kata Pengantar | vi |
| Abstract | vii |
| Abstraksi | viii |
| Daftar Isi..... | ix |
| Daftar Tabel | xi |
| Daftar Gambar..... | xii |
| Akronim | xiii |
| Motto | xvi |
| Halaman Persembahan..... | xviii |
| Ucapan Terimakasih..... | xix |
| BAB I: PENDAHULUAN..... | 1 |
| 1.1 Latar Belakang Masalah..... | 1 |
| 1.2 Rumusan Masalah | 7 |
| 1.3 Tujuan dan Manfaat Penulisan..... | 7 |
| 1.3.1 Tujuan Penulisan | 7 |
| 1.3.2 Manfaat Penulisan | 7 |
| 1.4 Penelitian Terdahulu | 8 |
| 1.5 Kerangka Konsep | 17 |
| 1.5.1 <i>Cyber War</i> | 17 |
| 1.5.2 <i>Network Security</i> | 25 |
| 1.6 Metodologi Penelitian | 29 |
| 1.6.1 Jenis Penelitian | 29 |
| 1.6.2 Metode Analisa Data | 29 |
| 1.6.3 Ruang Lingkup Penelitian | 30 |
| 1.6.4 Teknik Pengumpulan Data | 30 |
| 1.7 Asumsi Dasar | 31 |
| 1.8 Sistematika Penulisan | 31 |
| BAB II: SERANGAN HACKING CHINA PADA JARINGAN CYBERSPACE | |
| AMERIKA SERIKAT | 34 |
| 2.1 Sejarah Pendirian Teknologi <i>Cyber China</i> | 35 |
| 2.2 Tujuan <i>Cyber Attack China</i> | 41 |
| 2.3 Tipe <i>Cyber Threat China</i> | 45 |

| | |
|---|------------|
| BAB III: ANCAMAN CYBER ATTACK CHINA TERHADAP CYBER SECURITY AMERIKA SERIKAT | 48 |
| 3.1 Pembangunan Cyber Teknologi Sebagai Persiapan Cyber War China | 49 |
| 3.1.1 <i>Space and Counterspace Capabilities</i> | 49 |
| 3.1.1.1 <i>China Anti Satellite Technology (ASAT)</i> | 49 |
| 3.1.2 <i>Development in China Asymmetric Capabilities</i> | 59 |
| 3.1.2.1 <i>Online Blue Army China</i> | 59 |
| 3.1.2.2 PLA Unit 61398 | 64 |
| 3.1.2.3 <i>Computer Network Operation (CNO) Infrastructure</i> | 67 |
| BAB IV: PENINGKATAN CYBER SECURITY AMERIKA SERIKAT | 73 |
| 4.1 Kerugian-Kerugian Amerika Serikat dari Cyber Attack China | 73 |
| 4.2 Respon Amerika Serikat Untuk Meningkatkan Cyber Security | 79 |
| 4.2.1 Pembentukan USCYBERCOM (<i>United States Cyber Command</i>) | 79 |
| 4.2.2 Peningkatan Anggaran Cyber Security Amerika Serikat | 83 |
| 4.2.3 Pembentukan <i>United States Computer Emergency Readiness Team (US-CERT)</i> oleh DHS | 89 |
| 4.2.4 Pembentukan <i>National Strategy for Trusted Identities in Cyberspace (NSTIC)</i> | 94 |
| 4.2.5 Pembentukan Sistem Deteksi Intrusi | 98 |
| 4.2.5.1 EINSTEIN Program | 98 |
| BAB V: PENUTUP | 103 |
| 5.1 Kesimpulan | 103 |
| 5.2 Saran | 104 |
| DAFTAR PUSTAKA | 105 |

DAFTAR TABEL

| | |
|----------------------------------|----|
| 1.1 Tabel Posisi Penelitian..... | 17 |
|----------------------------------|----|



DAFTAR GAMBAR

| | |
|---|----|
| 4.1 CYBERCOM <i>structure</i> | 66 |
| 4.2 Infrastruktur kritis AS yang terhubung dengan <i>cyberspace</i> | 70 |
| 4.3 Pengeluaran anggaran TI AS..... | 71 |
| 4.4 Peningkatan anggaran <i>cyber security</i> pada DHS dan DOD..... | 72 |
| 4.5 US-CERT <i>structure</i> | 77 |



DAFTAR PUSTAKA

- **Buku:**

- deLisle, Jacques. Tun-Jen Cheng. et. al. 2006. *CHINA UNDER HU JINTAO: Opportunities, Danger and Dilemmas*. Singapore: World Scientific.
- Duncan, Sue and Wang Mingjie. 2006. *China 2006*. China: Foreign languages press.
- Kirshiner, Jonathan. 2006. *Globalization and National Security*. New York: Routledge.
- Taniputera, Ivan . 2011. *History of China*. Jogjakarta: Ar-Ruzz Media.
- Yan, Ke. 2004. *Science & technology in China reform and development*. China: China Intercontinental press.

- **E-Book**

- Lindsay, Jon R. Tai Ming Cheung & Derek S. Reveron. 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. New York: Oxford University Press.
http://longfiles.com/b72fx8qglwru/China_and_Cybersecurity_Espionage-Strategy-_and_Politics_in_the_Digital_Domain_ebook3000.pdf.html
- Tellis, Ashley J and Sean Mirski. 2013. *Crux of Asia: China, India and The Emerging Global Order*. Washington: Carnegie Endowment for International Peace. http://carnegieendowment.org/files/crux_of_asia.pdf
diakses tanggal 18-02-2016/pukul 19.57

- **E-Jurnal dan Working Paper**

- *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation: Prepare for The US-China Economic and Security Review Commission*, 2009, hal. 13.
<http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf>
diakses tanggal 18-02-2016/pukul 20.16
- Easton, Ian. *The Great Game In Space: China's Involving ASAT Weapons Programs and Their Implications for Future U.S. Strategy*. Project 2049 Institute.
http://project2049.net/documents/china_asat_weapons_the_great_game_in_space.pdf diakses tanggal 18-02-2016/pukul 20.00
- Federation of American Scientists. June 23, 2000. "*Chinese Anti-Satellite ASAT+ Capabilities*" diakses dari
<http://www.fas.org/spp/guide/china/military/asat/> dalam Amy Chang and USCC Research Fellow for Military & National Security Affairs. 2012. *Indigenous Weapons Development in China's Military Modernization*. U.S.-China Economic and Security Review Commission Staff Research Report. http://www.globalsecurity.org/military/library/report/2012/china-indigenous-military-developments_20120403.pdf diakses tanggal 07-05-2016/pukul 07.53
- Fritz, Jason. 2008. *How China Will Use Cyber Warfare to Leapfrog In Military Competitiveness*. Culture Mandala.
<http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm>
- Grego, Laura. 2012. *A History of Anti-Satellite Programs*. UCS (Union for Concernet Scientists) Global Security Program.
<http://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/a->

[history-of-ASAT-programs_lo-res.pdf](#) diakses tanggal 07-05-2016/pukul 07.53

- Kelso, T.S. 2007. *Analysis of the 2007 Chinese ASAT Test and the Impact of its Debris on the Space Environment*, Center of Space Standards & Innovation. <https://celestrak.com/publications/AMOS/2007/AMOS-2007.pdf> diakses tanggal 18-02-2016/pukul 20.06
- Lindsay, Jon R. 2015. *Exaggerating The Chinese Cyber Threat*. Quarterly Journal: International Security. Cambridge: Belfer Center for Science and International Affair. <http://belfercenter.ksg.harvard.edu/files/lindsay-china-cyber-pb-final.pdf>
- Mackey, James. 2009. *Recent US and Antis Satellite Activities*. USAF. <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj09/fal09/mackey.html>. Diakses tanggal 26-05-2015.
- Mardianis. 2012. Analisis Peristiwa Penembakan Satelit oleh China Dengan Menggunakan Teknologi Anti Satellite System (ASAT) Berdasarkan Hukum Internasional. http://jurnal.lapan.go.id/index.php/jurnal_asis/article/download/1774/1609 diakses tanggal 07-05-2016/pukul 07.53
- *Military Power of the People's Republic of China 2009*, 2009, Annual Report to Congress. Department of Defense. http://www.defense.gov/Portals/1/Documents/pubs/China_Military_Power_Report_2009.pdf diakses tanggal 18-02-2016/pukul 20.10
- Murray, Craig. 2013. *China Missile Launch May Have Tested Part of a New Anti-Satellite Capability*. <http://www.uscc.gov/sites/default/files/Research/China%20Missile%20La>

- [unch%20May%20Have%20Tested%20Part%20of%20a%20New%20Anti-Satellite%20Capability_05.22.13.pdf](#) diakses tanggal 18-02-2016/pukul 20.08
- Meisitha, Nadya Vira. 2014. Motivasi China Menguasai *Cyber* Teknologi. Hubungan Internasional. FISIP. Universitas Jember (UNEJ). <http://repository.unej.ac.id/bitstream/handle/123456789/59035/Nadya%20Vira%20Meisitha.pdf?sequence=1> diakses tanggal 18-02-2016/pukul 20.40
 - Kuehl, Daniel T. “*From Cyberspace to Cyberpower: Defining the Problem*”. cited, 38, dalam Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds.. *Cyberpower and National Security* (Washington, D.C.: National Defense UP, 2009) dalam Joseph S. Nye. 2010. *Cyber Power*. Cambridge: Belfer Center for science amd international affairs. Harvard Kennedy School. <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>
 - Office of the National Counterintelligence Executive. 2009-2011. October 2011. *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Balance Economic Collection and Industrial Espionage*. 7–8, diakses http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf dalam Amy Chang. 2014. *Warring State China’s Cybersecurity Strategy*. CNAS (Center for a New American Security), diakses dalam http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang_report_010615.pdf
 - Pollpeter, Kevin. *China’s Space Robotic Arm Programs*. UC Institute on Global Conflict and Cooperation, dalam <http://escholarship.org/uc/item/2js0c5r8#page-2> diakses tanggal 07-05-2016/pukul 07.52

- Stokes, Mark A. Jenny Lin and L.C. Russell Hsiao. 2011. *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*. Project 2049 Institute, dalam https://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf diakses tanggal 18-02-2016/pukul 20.25

- Schreier, Fred. 2015. *On Cyberwarfare*. Geneva: DCAF (Democratic Control of Armed Forces), dalam <http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf>

- Spade, Jayson M. *Information as Power: China's Cyber Power and America's National Security*. <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf> diakses tanggal 18-02-2016/pukul 20.14

- Stoke, Mark A. and L.C. Russell Hsiao. 2012. *Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests*. Project 2049 Institute. <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-079.pdf> diakses tanggal 18-02-2016/ pukul 20.34

- Tellis, Ashley J. *Punching the U.S. Military's "Soft Ribs": China's Antisatellite Weapon Test in Strategic Perspective*. No.51. June 2007. Carnegie Endowment for International Peace. http://carnegieendowment.org/files/pb_51_tellis_final.pdf diakses tanggal 18-02-2016/pukul 20.04

- US Department of Defense. 2006. *The National Military Strategy for Cyberspace Operations*. GL-1 dalam Nils Melzer. 2011. *Cyberwarfare*

and International Law. UNIDIR (United Nation Institute for Disarmament Research) RESOURCES.

<http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf> diakses tanggal 18-02-2016/pukul 20.15

- Wortzel, Larry M. 2010. *China's approach to cyber operations: implications for the United States*. testimony before the Committee on Foreign Affairs, House of Representatives, diakses dari http://origin.www.uscc.gov/sites/default/files/Congressional_Testimonies/LarryWortzeltestimony-March2010.pdf dalam Tobias Feakin. 2013. *Enter The Cyber Dragon: Understanding Chinese intelligence agencies cyber capabilities*. Special Report. ASPI (Australian Strategic Policy Institute). https://www.aspi.org.au/publications/special-report-enter-the-cyber-dragon-understanding-chinese-intelligence-agencies-cyber-capabilities/10_42_31_AM_SR50_chinese_cyber.pdf
- Ying, Fu. 2013. *The US and China: a new kind of great power relationship?*. The Brookings Institution. www.brookings.edu/~media/events/2013/6/12%20us%20china%20fu%20ying/20130612_us_china_transcript.pdf dalam James A. Lewis and Simon Hansen. 2014. *China's Cyberpower: International and Domestic Priorities*. https://www.aspi.org.au/publications/chinas-cyberpower-international-and-domestic-priorities/SR74_China_cyberpower.pdf
- **Website**
 - *A New Policy Typology to Better Understand The Goals of China's Space Programme*. <http://www.thespacereview.com/article/1958/2> diakses tanggal 07-05-2016/pukul 07.50

- *ASM-135 Kinetic Energy Anti-Satellite (KE-ASAT)*.
http://www.globalsecurity.org/space/systems/ke_asat.htm diakses tanggal 07-05-2016/pukul 07.53
- Beech, Hannah. 2011. *Meet China's Newest Soldiers: An Online Blue Army*. <http://world.time.com/2011/05/27/meet-chinas-newest-soldiers-an-online-blue-army/> Tanggal 31/12/2014.
- Bodeen, Christopher. 2013. *Inside "Unit 61398": Portrait Of Accused Chinese Cyberspying Group Emerges*. HuffPost Tech. http://www.huffingtonpost.com/2013/02/20/inside-unit-61398_n_2722356.html
- *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation: Prepare for The US-China Economic and Security Review Commission*, 2009. <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf> diakses tanggal 18-02-2016/pukul 20.16
- *China's Blue Army of 30 Computer Experts Could Deploy Cyber Warfare on Foreign powers*. 2011. The Times, dalam <http://www.theaustralian.com.au/business/technology/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/story-e6frgakx-1226064132826>
- *China Confirms Existence of Elite Cyber-Warfare Outfit The "Blue Army"*, 2011. <http://www.foxnews.com/tech/2011/05/26/china-confirms-existence-blue-army-elite-cyber-warfare-outfit/>

- *China Military Admits Cyberwarfare Unit Exists.*
http://www.nbcnews.com/id/43189050/ns/technology_and_science-security/t/china-military-admits-cyberwarfare-unit-exists/

- *Design and Analysis Case Study 13: National High-Tech R&D (863) Program.* 2011. http://globalpolicy.iipcollaborative.org/wp-content/uploads/sites/5/2014/10/Framework_China-Case-study.pdf diakses 18-02-2016/pukul 19.45

- Ditjen Informasi dan Komunikasi Publik-Kementerian Kominfo. 2013. Manfaat Teknologi Informasi dan Komunikasi Tepat Guna. Monumen Pers Nasional. <http://mpn.kominfo.go.id/index.php/2013/07/01/manfaat-teknologi-informasi-dan-komunikasi-tepat-guna/> diakses tanggal 04-12-2013.

- Gertz, Bill. *China Launches Three ASAT Satellites.* <http://freebeacon.com/national-security/china-launches-three-asat-satellites/> diakses tanggal 07-05-2016/pukul 07.52

- *Huanqiu Online. "Hong Kong Media: China's Cyberwar Army Applies Mao Zedong's War Tactics".* August 4. 2011. http://china.huanqiu.com/eyes_on_china/military/2011-08/1875446.html dalam *China's Cyberwarfare*. 2011. CHINASCOPE Analysis Series.

- Jiawei, Zhang. 2011. *China Confirms Deployment of Online Army.* http://www.chinadaily.com.cn/china/2011-05/26/content_12583698.htm

- Jie, Su. 2012. *PLA "Online Blue Army" Get Ready for Cyberwarfare.* www.ecns.cn/2012/01-16/6254.shtml

- Jones, Terril Yue. Bill Trott and Rob Taylor. 2013. *Chinese Hackers Steal U.S. Weapons Systems Designs, Report Says*. <http://usnews.nbcnews.com/news/2013/05/28/18556787-chinese-hackers-steal-us-weapons-systems-designs-report-says> diakses tanggal 29-05-2014.
- Lin, Zeo. 2014. *What we know about the Chinese army's alleged cyber spying unit*. CNN. <http://edition.cnn.com/2014/05/20/world/asia/china-unit-61398/> diakses tanggal 15-01-2016/pukul 19.30
- McGregor, James. *China's Drive for "Indigenous Innovation" A Web of Industrial Policies*. https://www.uschamber.com/sites/default/files/legacy/reports/100728chinareport_0.pdf diakses 18-02-2016/pukul 19.35
- *Science and Technology Programme in China*. 2003. <http://www.chinaconsulatesf.org/eng/kj/kjih/t43943.htm>
- Tadjdeh, Yasmin. 2014. *New Chinese Threats to U.S. Space Systems Worry Officials*. <http://www.nationaldefensemagazine.org/archive/2014/July/Pages/NewChineseThreatstoUSSpaceSystemsWorryOfficials.aspx> diakses tanggal 07-05-2016/pukul 07.48
- Tan, Francis. 2011. *China Admits Existence of a cyber-Warfare team a called "Blue Army"*. <http://thenextweb.com/asia/2011/05/30/china-admits-existence-of-a-cyber-warfare-team-called-blue-army/>
- Tantangan China Kepada AS Lewat Penguasaan Teknologi Militer. <http://jakartagreater.com/tantangan-china-kepada-lewat-penguasaan-teknologi-militer-3/> diakses tanggal 11-01-2016/pukul 14.30

- Thornburgh, Nathan. 2005. *"The Invasion of Chinese Cyberspies"*. August 26. The Time, available at <http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency> (accessed on April 05, 2012) dalam Rahul Prakash. 2013. *China and Cyberspace*. ORF (Observer Research Foundation) ISSUE BRIEF, hal. 03. http://www.orfonline.org/wp-content/uploads/2013/04/IssueBrief_52b.pdf
- Weeden, Brian. 2013. *Anti-Satellite Test in Space: The Case of China*. swfound (Secure World Foundation). http://swfound.org/media/115643/china_asat_testing_fact_sheet_aug_2013.pdf diakses tanggal 18-02-2016/pukul 20.01
- *What is Cryptology*. <http://www.wisegeek.com/what-is-cryptology.htm> diakses tanggal 13-02-2016/pukul 20.00
- Yu, Eileen. 2011. *China dispatches online army*. <http://www.zdnet.com/article/china-dispatches-online-army/>
- Zissis, Carin. 2007. *China's Anti-Satellite Test*. <http://www.cfr.org/china/chinas-anti-satellite-test/p12684> diakses tanggal 26-04-2015.